Amendments to the claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method to secure an electronic assembly having a processor and a storage means implementing a calculation process that calculates the result of a calculation that includes an elementary operation f(x) of a cryptography algorithm without performing the calculation f(x) thereby avoiding analysis of the operation of the electronic assembly using knowledge of the calculation f(x) and implementing a verification function used to perform an additional calculation on an intermediate result in order to obtain a calculation signature, the method comprising:

~~operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;~~

operating the processor of the electronic assembly according to instructions stored in the storage means to ~~perform the calculation of~~ obtain the result of the elementary operation f(x) by performing a modified calculation in lieu of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' in a set F, wherein x is a member of E and f(x) is a member of the set F; and

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional ~~the~~ calculation by ~~the~~ a verification function using the result obtained by the super function in order to obtain ~~the~~ a calculation signature.

2. (Previously Presented) The method according to claim 1, wherein the method further comprises:
operating the processor of the electronic assembly according to instructions stored in the storage means to perform at least once more all or part of the calculation in order to recalculate said signature and compare them in order to detect a possible error.

3. (CANCEL)

4. (Previously Presented) The method according to claim1, wherein the calculation of the elementary operation can be recomputed using the calculation of the super-function.

5. (Previously Presented) The method according to claim 1, further comprising operating the processor of the electronic assembly according to instructions stored in the storage means to

move from E to E' by one-to-one function h_1; and

move from F' to F by onto function h_2;

wherein h_1 and h_2 are mappings such that for any element x of E the following equality is true: $h_2(f'(h_1(x)))=f(x)$.

6. (Currently Amended) An electronic assembly secured from differential attack and comprising a calculation process processing means that

includes performing a calculation that includes an elementary operation f(x) of a cryptography algorithm, wherein the electronic assembly comprises storage means for storing instructions to cause the calculation processing means to execute a verification function used to perform an additional calculation on intermediate results in order to obtain a calculation signature thereby securing the electronic assembly from differential attack; and

wherein the calculation process comprises:

~~operating the calculation processing means of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;~~

operating the processor of the electronic assembly according to instructions stored in the storage means to ~~perform the calculation of~~ obtain the result of the elementary operation f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F; and

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional ~~the~~ calculation by ~~the~~ a verification function using the result obtained by the super function in order to obtain ~~the~~ a calculation signature.

7. (CANCEL)

8. (Previously Presented) A smart card comprising storage means of a

calculation process, processing means of said process, wherein the smart card includes storage means storing instructions implementing a calculation process that calculates the result of a calculation that includes an elementary operation f(x) of a cryptography algorithm without performing the calculation f(x) thereby avoiding analysis of the operation of the electronic assembly using knowledge of the calculation f(x) and implementing ~~of~~ a verification function used to perform an additional calculation on an intermediate result ~~results~~ in order to obtain a calculation signature; and

wherein the calculation process comprises:

~~operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;~~

operating the processor of the electronic assembly according to instructions stored in the storage means to ~~perform the calculation of~~ obtain the result of the elementary operation f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F; and

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional ~~the~~ calculation by ~~the~~ a verification function using the result obtained by the super function in order to obtain ~~the~~ a calculation signature.

9. (Previously Presented) The method according to claim 2, wherein the calculation of the elementary operation can be recomputed using the calculation of the super-function.

10. (new) The method according to Claim 1, wherein the elementary operation f(x) is a substitution function of a DES cryptography algorithm.

11. (new) The electronic assembly according to Claim 6, wherein the elementary operation f(x) is a substitution function of a DES cryptography algorithm.

12. (new) The smart card according to Claim 1, wherein the elementary operation f(x) is a substitution function of a DES cryptography algorithm.